KONGERIKET NORGE
The Kingdom of Norway

REC'D 28 JAN 2004
WIPO PCT

PCT/NO03/445

Bekreftelse på patentsøknad nr
Certification of patent application no

20026284

Det bekreftes herved at vedheftede dokument er nøyaktig utskrift/kopi av ovennevnte søknad, som opprinnelig inngitt 2002.12.30

It is hereby certified that the annexed document is a true copy of the above-mentioned application, as originally filed on 2002.12.30

2004.01.09

Line Reum

Line Reum
Saksbehandler

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

PATENTSTYRET
Styret for den industrielle rettsvern

BL. 130 - 5.000 - 01.2001 - Hegro Grafisk AS

PATENTSTYRET
02-12-30*20026284

PATENTSØKNAD

Søker:

Thor I. Fossen
Marine Cybernetics AS
Postboks 4607
7451 TRONDHEIM

Oppfinnere:

Olav Egeland, *Marine Cybernetics AS*
Thor I. Fossen, *Marine Cybernetics AS*
Tor Arne Johansen, *Marine Cybernetics AS*
Asgeir J. Sørensen, *Marine Cybernetics AS*

Jon Rysst, *Det Norske Veritas AS*
Tor E. Svensen, *Det Norske Veritas AS*

Oppfinnelsens benevnelse:

Metode for testing og sertifisering av datamaskinbaserte styre- og overvåkningssystemer over en kommunikasjonskanal

METODE FOR TESTING OG SERTIFISERING AV DATAMASKINBASERTE STYRE- OG OVERVÅKNINGSSYSTEMER OVER EN KOMMUNIKASJONSKANAL

Sammendrag

Oppfinnelsen går ut på å sertifisere (*CyberCertification*) et styre- og overvåkningssystem basert på fjerntesting (remote testing) av systemet i sann tid mot et simulert fysisk system under simulerte feilsituasjoner, eksterne forstyrrelser og målestøy. Den foreliggende oppfinnelsen beskriver en fremgangsmåte eller metode hvor testing av styre- og overvåkningssystemet gjøres ved å koble det opp mot en hardware-in-the-loop simulator ved hjelp av en eller flere kommunikasjonskanaler. Dette gjøres i sann tid slik at feilsituasjoner kan testes og brukes som underlag for *CyberCertification*. Systemets tidsresponser og statussignaler blir sendt over en kommunikasjonskanal for presentasjon til testoperatøren og lagring for senere analyse (figur 1).

Oppfinnelsens område

Den foreliggende oppfinnelsen vedrører en fremgangsmåte eller metode for fjerntliggende testing av styre- og overvåkningssystemer (reguleringssystemer) over en eller flere kommunikasjonskanaler (figur 1). Testingen foregår ved at styresystemet sender signaler over en kommunikasjonskanal (GSM, telefon, radiosamband m.m) i sann tid til en *hardware-in-the-loop* (HIL) simulator som returnerer en simulert respons og statussignaler til et fysisk system, inkludert farkost, reguleringssytem, sensorer og aktuatorer.

I tillegg vedrører oppfinnelsen en fremgangsmåte eller metode for sertifisering av styre- og overvåkningssystemer basert på testing av systemet i sann tid mot et simulert fysisk system under simulerte feilsituasjoner, eksterne forstyrrelser (som vær og vind) og støy. Dette blir heretter kalt *CyberCertification*.

Anvendelseområde

Metoden har anvendelse for alle marine farkoster deriv undervannsfartøyer, torpedoer, fritt flytende fartøyer som skip, hurtigbåter, plattformer osv. samt forankrete fartøyer. Konseptet kan også brukes til å teste og sertifisere styresystemer for fly, satellitter, biler, motorer, prosesstyringssystemer, mekaniske systemer osv.

Formålet med å teste datamaskinbaserte styre- og overvåkningssystemer mot en HIL-simulator via en sanntids kommunikasjonskanal er at simulatoren og operatøren kan lokaliseres langt fra styre-/overvåkningssystemet. Dette muliggjør fjerntliggende testing (eng: *remote testing*) og sertifisering av reguleringssystemer. Ulike feilsituasjoner definert av en testoperatør og sertifiseringsmyndigheter genereres i simulatoren som kommuniserer direkte med styre- og overvårkingssystemet. Responsen på disse sendes tilbake til testoperatøren som vist i figur 1. Metoden kan også benyttes med lokal kommunikasjon og samlokalisering av simulator og reguleringssystem.

Kjente metoder

Sertifisering av styre- og overvåkningssystemer for marine anvendelser utføres i dag først etter installasjon av systemet om bord i selve fartøyet. Dette prinsippet forutsetter at styre- og overvåkningssystemet er lokalisert om bord i fartøyet hvor det er koblet sammen med den fysiske prosessen via kabler. Fartøyet må være i drift for å utføre testen. Slike tester er begrenset av tilgjengelig tid, gitte værforhold, og dekker kun et lite antall feilsituasjoner.

Hensikten med oppfinnelsen

Hovedhensikten med oppfinnelsen er å muliggjøre fjerntliggende testing og sertifisering av datamaskinbaserte styre- og overvåkningssystemer. En ny fremgangsmåte eller metode for fjerntliggende testing av styre- og overvåkningssystemer over en kommunikasjonskanal gjør at testing/sertifisering kan utføres uten at operatøren er lokalisert på samme sted som styre- og overvåkningssystemet (figur 1).

En annen hensikt med fjerntesting er at man får mye større fleksibilitet til å teste programvare og systemet som helhet under simulerte feilsituasjoner og mer omfattende spektrum av værbelastninger enn hva som er tilfellet under konvensjonell testing/sertifisering.

Ytterligere hensikter ifølge oppfinnelse går ut på å gi anvising på en metode der man unngår de ulemper og begrensninger som tidligere kjente metoder er beheftet med.

Figurbeskrivelse

Figur 1 viser en prinsippskisse for fjerntliggende testing og sertifisering (*CyberCertification*) av styre- og overvåkningssystemer. Testoperatøren samt sertifiserende myndigheter er lokalisert i kontrollrommet som er utstyrt med en dynamisk HIL-simulator. Simulatoren er koblet til en eller flere kommunikasjonskanaler som opererer i sann tid.

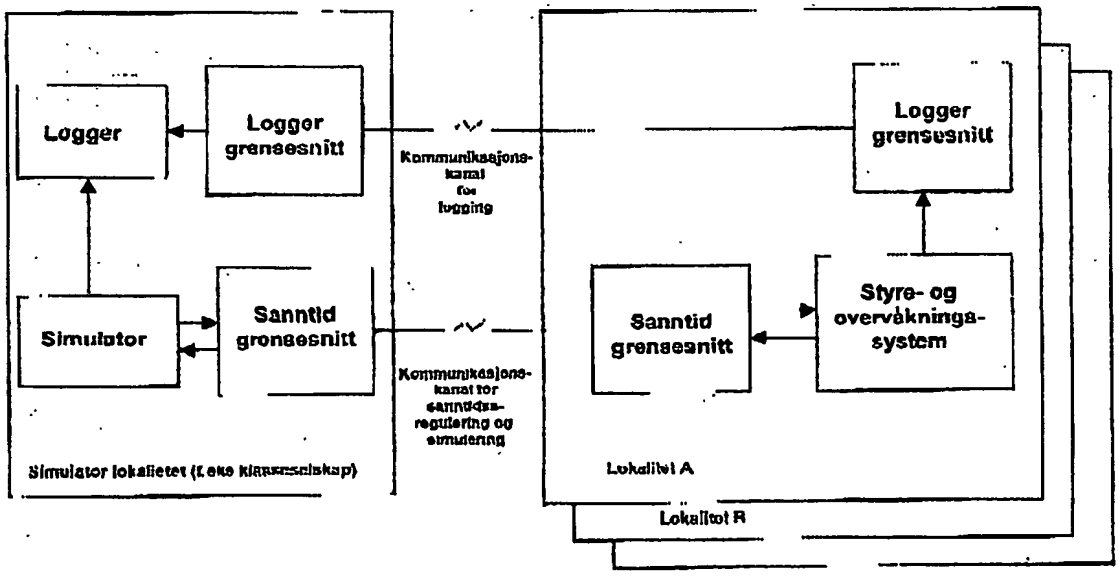
I simulatorlokalitet er simulatoren og datalogger. Dataloggeren registrerer reguleringssystemets statussignaler, feilmeldinger, alarmer og tidsresponser fra simulator, styre- og overvåkningssystemet. Dataloggeren er koblet til en kommunikasjonskanal som oversender signaler.

Styre- og overvåkningssystemene er lokalisert i lokalitetene A, B,....osv. Systemene er koblet sammen med simulatoren ved hjelp av en programmerbar kommunikasjonsenhet.

Styre- og overvåkningssystemet er også koblet sammen med dataloggeren i simulatorlokaliteten ved hjelp av en kommunikasjonskanal. Denne overfører viktige data som statussignaler, feilmeldinger, alarmer og tidsresponser som brukes som underlag for *CyberCertification*.

Patentkrav

1. En metode eller fremgangsmåte for fjerntliggende testing av styre- og overvåkningssystemer (reguleringssystemer) over en eller flere kommunikasjonskanaler som beskrevet ovenfor. Testingen foregår ved at styresystemet sender signaler over en kommunikasjonskanal (GSM, telefon, radiosamband m.m) i sann tid til en *hardware-in-the-loop* (HIL) simulator som returnerer en simulert respons og statussignaler til et fysisk system, inkludert farkost, reguleringssytem, sensorer og aktuatorer. HIL-simulatoren benytter i og for seg kjente matematiske modeller for det fysiske systemet basert på dynamikk, fluidmekanikk, termodynamikk og elektroteknisk teori for beregning av bevegelse, belastninger og andre kritiske variable. Feilsituasjoner og ytelse testes ved inn- og utkobling av delsystemer (simulering av sammenbrudd av komponenter), forandring/generering av forstyrrelser, eksterne forstyrrelser som vær og vind, elektrisk støy osv. Metoden for fjerntliggende testing omfatter også dynamisk rekonfigurering av det datatekniske grensesnittet ved at ny programvare overføres fra simulatorlokalitet til datamaskinen inne i enheten. Systemet kan derfor tilpasses ulike styre- og overvåkningssystemer levert av firma A, B,....osv. (figur 1).
2. En metode i henhold til krav 1 for sertifisering (som definert av klasseselskap f.eks. Det Norske Veritas AS) av styre- og overvåkningssystemer basert på testing av systemet i sann tid mot et simulert fysisk system under simulerte feilsituasjoner, eksterne forstyrrelser (som vær og vind) og støy.



Figur 1. Prinsippskisse som viser konseptet for CyberCertification.